Reliability Analysis of Renewable Redundant Systems with Unreliable Monitoring and Switching

Yakov Genis
Borough of Manhattan Community College
City University of New York
USA
ygenis@bmcc.cuny.edu

Igor Ushakov
Canadian Training Group, San Diego
USA
iushakov@mail.com

Abstract

Two methods of approximate evaluation of probability of no-failure operation and maintainability of renewable redundant system is suggested. The model takes into account incomplete monitoring of units state and not absolutely reliable switching device. Fast restoration, fast unit failure detection and fast standby switching are assumed.

1. Introduction

Delays in unit failure detection and "false" failure diagnosis substantially reduce redundant systems reliability. To find the actual system reliability, one must take into account all factors associated with imperfect testing, and unreliable switching. The reliability of such systems was analyzed in *Ushakov (1994)*. Some specific cases are considered in *Genis (1988)* and *Genis (1989)* that are further developed below along with heuristic methods suggested in *Gnedenko and Ushakov (1995)*.

2. Problem Statement

A renewable redundant system contains n units and r repair facilities (RF). The distribution function (DF) of time to failure for each unit is assumed exponential. A unit might be in operational or failed states. The monitoring imperfectness may delay detection of a unit failure. At the same time, it is possible false unit failure detecting.

In system with standby redundancy (SR), after an active unit failure, its function is performed by a standby unit. Switching device itself is not absolutely reliable.

As soon as a unit failure, real or false, is detected, the renewal of this unit begins. The system is assumed to be provided with fast servicing (FS) that means that the unit idle time is much less than the time between failures as it defined in *Genis (1989)*.

There is no restrictions to the structure of the system. The system is said to fail if the domain of the states of its units belongs to a specified set of states. The problem is to estimate the reliability and availability indexes of the system with FS.

3. Asymptotic Approach. General System Model.

The state of system units is assumed to belong to a malfunction interval (MI) if even one of its units is in a state of detected, undetected, or false failure and to a serviceable interval (SI), otherwise. An MI is called a failure MI if system failure occurs within this interval. It means that in this MI at least once the system will exhaust its reliability reserve. The system can fail in some MI more than once. System behavior is described by an alternating random process in which MIs and SIs follow each other. The behavior of such system has been analyzed in *Genis (1989)*.

Let us assume that the system operating conditions and the units no-failure operation time and restoration time DF do not change with time. The system to be discussed is assumed to be highly reliable. Since the probability of failure of such a system in its nonstationary operation region can be made small enough, its behavior in the stationary operation region becomes of primary importance. The results of *Genis (1989)* indicate that in such a case the DF of the time to first system failure converges to an exponential function if the product of the rate of occurrence of MIs λ by the maximum mean duration of the malfunction interval T as well as the probability of system failure q in the MI interval tends to zero. If also the probability q^* of more than one system failure taking place in the MI tends to zero, the DF of the time between two consequent system failures converges to an exponential function. The FS criterion defined below ensures conditions in which $\lambda T \to 0$, $q \to 0$ and $q^* \to 0$.

\7

4. Refined System Model and the FS Criterion

Consider a system with with SR. Let $F_i(x)$ and m_i be respectively the DF and the mean of time to failure of the *i*-th unit. The probability of instantaneous detection of the *i*-th active unit failure is p_{1i} and that of the *i*-th standby unit is p_{2i}. When a failure of an *i*-th active unit is detected the probability of instantaneous switching to a standby unit is p_{3i}; let $H_i(x)$ denote the DF of switching time to the standby when a failure of the *i*-th active unit is detected and the switching is not instantaneous.

An undetected failure of an *i*-th unit can be found in the course of periodic tests with a probability p_{4i}; the distribution function, mean time between two PTs, and its second moment are denoted by $\Phi(x)$, m_{pt}, and $m_{pt}^{(2)}$ respectively. The DF of the time from the beginning of an MI to the first PT after the MI begun is given by

$$\Phi_1(x) = \frac{1}{m_{pt}} \int_0^x \bar{\Phi}(u)du, \text{ and } m_{pt1} = \int_0^\infty \bar{\Phi}_1(x)dx = \frac{m_{pt}^{(2)}}{2m_{pt}}$$

Here and below $\bar{\Gamma} = 1 - \Gamma$ for all Γ. The DF of the time to detect the failure of *i*-th unit under the condition of not instantaneous detection of this failure is $B_i(x)$, and its mean is given by

$$m_{ki} = \int_0^\infty \bar{B}_i(x)dx = \left(m_{pt}^{(2)} / 2(m_{pt})^2 + \bar{p}_{4i} / p_{4i} \right) m_{pt} .$$

The probabilities of a false signal being generated to indicate a no existing failure of a serviceable active and standby unit are p_{5i} and p_{6i} respectively. Let $G_i(x)$ is the DF of the restoration time of the *i*-th failed unit and $G_{1i}(x)$, an analogous function when a false failure of the *i*-th unit is indicated.

In addition, let s be the minimum number of _units whose failure causes system failure; $\bar{G}(x) = \max \bar{G}_i(x)$, $\bar{H}(x) = \max \bar{H}_i(x)$, $\bar{B}(x) = \max \bar{B}_i(x)$, where $i \in \overline{1,n}$; $m_r^{(j)}$, $m_{1r}^{(j)}$, $m_s^{(j)}$, and $m_k^{(j)}$ are the *j*-th moments of the DF $G(x)$, $G_1(x)$, $H(x)$, and $B(x)$; and let $m_r = m_r^{(1)}$, $m_{1r} = m_{1r}^{(1)}$, $m_s = m_s^{(1)}$, $m_k = m_k^{(1)}$.

Under stationary system operating conditions the rate of occurrence of MIs is estimated as

$$\tilde{\lambda} \leq \max \left\{ \sum_{i=1}^{n} \max(p_{5i}, \; p_{6i}) / m_{pt}, \; \sum_{i=1}^{n} 1/m_i \right\}.$$

In practically important cases $m^{(j)} \leq C(m)^j$ (subscripts omitted), and for small s $\approx$ 2-3, the FS condition *Genis (1989)*] can be written as

$$\alpha_1 = \tilde{\lambda} \; \max(m_r, m_{1r}, m_s, m_k) \to 0,$$

and for systems with SR an additional condition is

$$\alpha_2 = \max_{1 \leq i \leq n} p_{1i} \to 0, \qquad \alpha_3 = \max_{1 \leq i \leq n} \bar{p}_{3i} \to 0 .$$

The obtained reliability estimates are valid when $\alpha = \max(\alpha_1$, aα_2, $\alpha_3) \leq 0.1$ since their error is of the same order as α .

5. Estimates of Reliability and Maintainability Indexes

A failure in which a system persists for at least a time *x* is called an *x*-failure, and let $\tilde{\beta}_x$ denote the rate or *x*-failures taking place in the system under stationary conditions. It can be shown that the desired reliability indexes can be found in terms of the $\tilde{\beta}_x$.

Under FS conditions the DF of system operating time to first failure, of the time between two failures, and of the no-failure operating time are nearly exponential. The mean time to failure and the mean time between failures can be assumed to be approximately equal to the mean no-failure operating time of the system. Then, assuming in $\tilde{\beta}_x$ x =0, we get the system failure rate $\tilde{\beta} = \tilde{\beta}_0$, the estimation of no-failure operating time $T \approx 1/\tilde{\beta}$, the estimation of DF no-failure operating time as l - exp {- $\tilde{\beta}$ }, the estimation of DF of system restoration time as 1 - $\tilde{\beta}_x / \tilde{\beta}$, and the estimation of mean system restoration time in the form of the $\int_0^\infty \tilde{\beta}_x / \tilde{\beta} \; dx$.

Under FS conditions $\tilde{\beta}_x$ is found as the sum of x-failure rates of the system along monotonous paths *Genis (1989)*, i.e., paths along with no single restoration can be completed during the time from the beginning of the MI until system failure on this interval plus the time *x*; SR system requires in addition that no single standby switching can be completed and no single active unit failure is no instantaneously detected during that time.

The rate of x-failures along some monotonous path is defined as the product of the rate of occurrence of MIs at which a given path can start and the probability of x-failure along this path. The obtained estimates are then simplified in accordance with the results obtained in *Genis (1988)*.

To simplify the calculation of estimates only minimal monotonous paths are used on which the probability of system failure is substantially greater than on nonminimal paths. Other conditions being equal, the number of failed units that cause system failure is the least along minimal paths. Thus, in case of instantaneous switching of standby units and instantaneous detection of active unit failures, one only takes into account those paths along which system failure takes place with the failure of *s* units. In case of noninstantaneous standby switching or noninstantaneous active unit failure detection, only those paths are taken into account along which the noninstantaneous switching or noninstantaneous detection takes place with failure of the first unit in this MI.

If only the system reliability indexes are needed then the b' can be found immediately. It should be also noted that the rate of *x*-failures b'_x of a system can be used to estimate the reliability indexes of systems with time redundancy.

The obtained results can be probably extended to the case when the DF $F_i(x)$ are absolutely continuous. In this case the rate of the occurrence of MIs in stationary system operation can be estimated by value

$$l' \leq \max \left\{ \sum_{i=1}^{n} \max(p_{5i}, \ p_{6i}) \ / \ m_{pt}, \quad \sum_{i=1}^{n} \max(1/m_i, c_i) \right\},$$

where c_i is the value at the zero of density of $F_i(x)$, $c_i = F_i'(0)$.

The above method is illustrated with the following examples in which the approximate estimates have been found to be close to either exact values or to values obtained by simulation.

Several particular illustrative examples are considered.
(1) Unloaded duplicate system with non-reliable switching.

(2) Loaded redundant system with non-instantaneous switching and non-instantaneous failure detection of redundant unit.

6. Heuristic approach

The idea of approximate method is based on the Renyi Theorem that states that infinitely repeating "sifting procedure" leads in limit to a Poisson process. In our case, for each system unit, we consider a recurrent alternative processes consisting of "on-intervals" with DF $F(t)$ and the mean T, and "down-intervals" with DF $G(t)$ and the mean t. In our case, considering highly reliable system, we take $T >> t$. Let us call a unit failure an "alarm", if it can be developed into a system failure if another failure (or other failures) will occur. Notice that such situation exists for a very short time, since we assume that $T >> t$. So, in limit, we can consider pure recurrent point process of "alarms" instead of alternating one. Sometimes these alarms might develop into system failures, sometimes not.

Several illustrative examples are given for demonstration of the suggested heuristic method.

REFERENCES

Genis, Y. (1989). 2-sided estimates for the reliability of a renewable system under a non-stationary operational regime. *Soviet Journal of Computer And Systems Sciences*, 27(6), 168-170.

Genis, Y (1988). Indexes of suitability for repair and the coefficient of readiness of standby systems for various renewal disciplines. *Soviet Journal of Computer and Systems Sciences*, 26(3), 164-168.

Gnedenko, B., and I. Ushakov (1995). *Probabilistic Reliability Engineering*. John Wiley & Sons, N.Y.

Ushakov, I., *Ed.* (1994) *Handbook of Reliability Engineering*. John Wiley & Sons, N.Y